|  |  |
| --- | --- |
|  | **CASTLE DONINGTON PARISH COUNCIL**Community Hub, 101 Bondgate, Castle Donington, Derby. DE74 2NR**Telephone (01332) 810432****Email: admin@cdpc.org.uk**Clerk: Fiona M. Palmer |

# **Barclaycard Information Security Policy**

### **Introduction**

This Policy Document encompasses all aspects of security surrounding confidential information and must be distributed to all employees of both the Parish Council and Volunteer Centre. Everyone must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by Parish Council on an annual basis or when relevant to include newly developed security standards into the policy and distribute it all employees as applicable.

The Model document from Barclaycard was reviewed, and a discussion held with an advisor of Barclaycard, who said that a policy based on what is relevant to the Parish Council was more appropriate than the standard model document which was originally sent.

It was also advised that to ensure compliance with the Payment Card Industry Data Security Standard that the Parish Council should opt to upgrade from the Self-Assessment Data Security Manager service to the Proactive Security Service.

### **Information Security Policy**

Castle Donington Parish Council and the Volunteer Centre handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.

Castle Donington Parish Council and the Volunteer Centre commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end Castle Donington Parish Council and the Volunteer Centre are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Employees handling Sensitive Cardholder data should:

* Handle cardholder information in a manner that fits with their sensitivity.
* Limit personal use of Parish Council and Volunteer Centre information and telecommunication systems and ensure it doesn’t interfere with your job performance.
* Castle Donington Parish Council reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose.
* Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal.
* Do not disclose personnel information unless authorised.
* Protect sensitive cardholder information.
* Keep passwords and accounts secure.
* Request approval from the Parish Council prior to establishing any new software or hardware, third party connections, etc.
* Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval.
* Always leave desks clear of sensitive cardholder data and lock computer screens when unattended.
* Information security incidents must be reported, without delay, to the individual responsible for incident response locally – Please find out who this is.

We each have a responsibility for ensuring Parish Council and Volunteer Centre systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

### **Acceptable Use Policy**

The Parish Council’s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Parish Council established culture of openness, trust and integrity. The Parish Council is committed to protecting the employees, partners, councillors and Castle Donington Parish Council and the Volunteer Centre from illegal or damaging actions by individuals, either knowingly or unknowingly. Castle Donington Parish Council will maintain an approved list of technologies and devices and personnel with access to such devices as detailed in Appendix B.

* Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
* Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies
* Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
* Employees should ensure that technologies should be used and setup in acceptable network locations
* Keep passwords secure and do not share accounts.
* Authorized users are responsible for the security of their passwords and accounts.
* All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
* All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
* Because information contained on portable computers is especially vulnerable, special care should be exercised.
* Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Castle Donington Parish Council, unless posting is in the course of business duties.
* Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

### **Stored Data**

Castle Donington Parish Council and the Volunteer Centre **DO NOT** store any sensitive cardholder data.

**It is strictly prohibited to store:**

1. The contents of the payment card magnetic stripe (track data) on any media whatsoever.
2. The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
3. The PIN or the encrypted PIN Block under any circumstance.

### **Physical Security**

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

* Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
* Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies
* Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
* Employees should ensure that technologies should be used and setup in acceptable network locations
* A list of devices that accept payment card data should be maintained.
* The list should include make, model and location of the device
* The list should have the serial number or a unique identifier of the device
* The list should be updated when devices are added, removed or relocated

### **Security Awareness and Procedures**

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

### **Network security**

Firewalls must be implemented, and all security is managed in conjunction with Sc-It Solutions.

### **Anti-virus policy**

All machines must be configured to run the latest anti-virus software as approved by Castle Donington Parish Council. The preferred application to use is Panda Adaptive Defence Anti-Virus software, which must be configured to retrieve the latest updates to the antiviral program automatically on a daily basis. The antivirus should have periodic scanning enabled for all the systems

### **Security Incidents**

'Security incident' means any incident (accidental, intentional or deliberate) relating to your communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money, or just to damage your company.

Employees of Castle Donington Parish Council and the Volunteer Centre will be expected to report to the Clerk to the Parish Council for any security related issues.

### **Roles and Responsibilities**

* Castle Donington Parish Council and Volunteer Centre are responsible for overseeing all aspects of information security.
* Castle Donington Parish Council and Volunteer Centre should monitor and control all access to data.

# Appendix A

### **Agreement to Comply Form – Agreement to Comply with Information Security Policy.**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Employee Name (printed)**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Department**

* I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to Castle Donington Parish Council and the Volunteer Centre by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with Castle Donington Parish Council and Voluenteer Centre, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the Clerk to the Council who is the designated information owner.
* I agree to abide by the policies and other requirements found in Castle Donington Parish Council security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.
* I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer, the Clerk to the Council.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Employee Signature**

# Appendix B

|  |  |  |  |
| --- | --- | --- | --- |
| **Asset/Device Name** | **Description** | **Owner/Approved User** | **Location** |
|  |  |  |  |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |